UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-15-05 Office of Audits October 2014

Audit of the Department of State Implementation and Oversight of Active Directory

~~**IMPORTANT NOTICE**: This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

(U) PREFACE

(U) This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

(U) This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

(U) The recommendations therein have been developed on the basis of the best knowledge available to OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

(U) I express my appreciation to all of those who contributed to the preparation of this report.

(U) Norman P. Brown
(U) Assistant Inspector General
for Audits

(U) Acronyms

(U) AD	Active Directory
(U) DS	Bureau of Diplomatic Security
(U) FAM	*Foreign Affairs Manual*
(U) FISMA	Federal Information Security Management Act
(U) HR	Bureau of Human Resources
(U) IRM	Information Resource Management
(U) ISSO	Information System Security Officer
(U) IT	information technology
(U) OIG	Office of Inspector General
(U) OU	organizational unit
(U) SBU	sensitive but unclassified

(U) Table of Contents

(U) Section **(U)** Page

(U) Executive Summary

(U) The U.S. Department of State (Department) uses Active Directory (AD), a directory service created by Microsoft for Windows domain networks, which provides the capability to centrally manage network users and system information while enforcing the Department's security standards and standardizing network configuration. One of AD's functions, Domain Services, allows an information technology (IT) administrator to manage network resources and organize elements of the network in a standardized structure. Another of AD's services, Rights Management, allows organizations to safeguard digital information from unauthorized use by allowing IT administrators[1] to define who in the organization can open, modify, or take other actions related to the information.

~~(SBU)~~ The Office of Inspector General (OIG) initially discovered deficiencies in AD account management during the FY 2010 Federal Information Security Management Act (FISMA) audit and during subsequent audits.[2] The objective of this audit was to determine whether the Department[3] has consistently implemented and overseen Active Directory Domain Services and Rights Management across the enterprise environment. See Appendix A for more information on OIG's audit scope and methodology.

~~(SBU)~~ OIG found that the Department's Bureau of Information Resource Management (IRM) has organized and successfully implemented AD Domain Services in a standardized structure, including Group Policy Objects[4] and trusts,[5] and put procedures in place to better ensure business continuity.[6] OIG also found, however, that IRM has not consistently implemented AD Rights Management, which is necessary to enforce IT security standards. OIG identified deficiencies in IRM's oversight of the management of user accounts that allowed thousands of unused accounts to remain active—posing a significant risk for unauthorized access

[1] **(U)** The label "IT administrators" is used within this report; however, Microsoft calls such administrators "content owners." Microsoft, *Windows Server*, technet.microsoft.com/en-us/library/cc771234(v=WS.10).aspx, accessed 8/26/2014.

[2] **(U)** OIG, AUD-IT-11-07, *Review of Department of State Information Security*, November 2010; AUD-IT-12-14, *Evaluation of the Department of State Information Security Program*, November 2011; AUD-IT-13-03, *Audit of Department of State Information Security Program*, November 2012; and AUD-IT-14-03, *Audit of Department of State Information Security Program*, November 2013.

[3] **(U)** The core design team for AD included members from the Executive Secretariat and the following Bureaus: Administration, Consular Affairs, Diplomatic Security, International Information Programs, and Information Resource Management.

[4] **(U)** Group Policy is an infrastructure that allows implementation of specific configurations for users and computers. Group Policy settings are contained in Group Policy objects, which are linked to sites, domains, or organizational units. Microsoft, *Windows Server*, technet.microsoft.com/en-us/windowsserver/bb310732.aspx, accessed 8/26/2014.

[5] **(U)** Trusts are authentication pipelines that must be present in order for users in one domain to access resources in another domain. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/cc775736(v=ws.10).aspx, accessed 8/26/2014.

[6] **(U)** Business Continuity is the capability of an organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business Continuity Institute, "What is BC?" www.thebci.org/index.php/resources/what-is-business-continuity, accessed 8/26/2014.

and use as well as unnecessary maintenance costs—and inconsistent and uncompliant organizational unit (OU)[7] structuring of AD accounts.

~~(SBU)~~ These deficiencies occurred because IRM had not established a governance structure to ensure that AD Rights Management was implemented and managed consistently. The Department's AD Rights Management is decentralized, allowing the Information Management Officers at each bureau or post to make decisions about implementing and overseeing AD accounts with insufficient guidance. Without a proper governance structure and guidance for AD Rights Management, the risk of unauthorized access or malicious activity on the network is significantly increased.

~~(SBU)~~ In its October 9, 2014, response to the draft report (see Appendix B), IRM requested that we clarify responsibility for managing AD at the Domain level and below. We modified the report to reflect the role and responsibility of the Information Management Officer in managing AD. IRM also commented on the six recommendations we offered to establish a governance structure for AD Rights Management and improve account management.[8] IRM concurred with five of the six recommendations and suggested that the Bureaus of Human Resources (HR) and Diplomatic Security (DS) be added as coordinating partners for two of the recommendations we offered. After consultation with HR and DS, we modified the recommendations to reflect HR and DS involvement in implementing the recommendations. Based on IRM's response to the recommendations, we consider five recommendations resolved, pending further action, and one recommendation unresolved because IRM did not indicate agreement or disagreement with the recommendation. A synopsis of IRM's response to each recommendation and OIG's reply is presented after each recommendation.

(U) Background

(U) AD is a directory service created by Microsoft for Windows domain networks and used by the Department since 2001. AD provides the means to centrally manage network users, groups, workstations/computers, servers, printers, network shares, and system information while enforcing the Department's security standards and standardizing network configuration. The implementation of AD provided the capability to assign access controls to individuals and services based on their respective roles.

(U) *Microsoft Best Practices* explains that AD's Domain Services function assists IT administrators in managing network resources and organizing elements of the network in a standardized structure. *Diplopedia*[9] further explains that AD allows IT administrators to organize the elements of the Department's network, such as users, workstations, and devices, into a

[7] **(U)** An organizational unit (OU) is an AD container in which users, groups, computers, and other organizational units may be placed. An organizational unit cannot contain objects from other domains. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/cc758565(v=WS.10).aspx, accessed 8/26/2014.

[8] **(U)** Account management is included because Rights Management allows IT administrators to define who can open, modify, or take other action with the information.

[9] **(U)** *Diplopedia* is an online encyclopedia, available to those with access to the Department's OpenNet system, which contains topics related to the Department's workforce.

hierarchical, tree-like structure. One part of the structure is a user object,[10] which has attributes such as first name, last name, work phone number, and group membership associated with it.

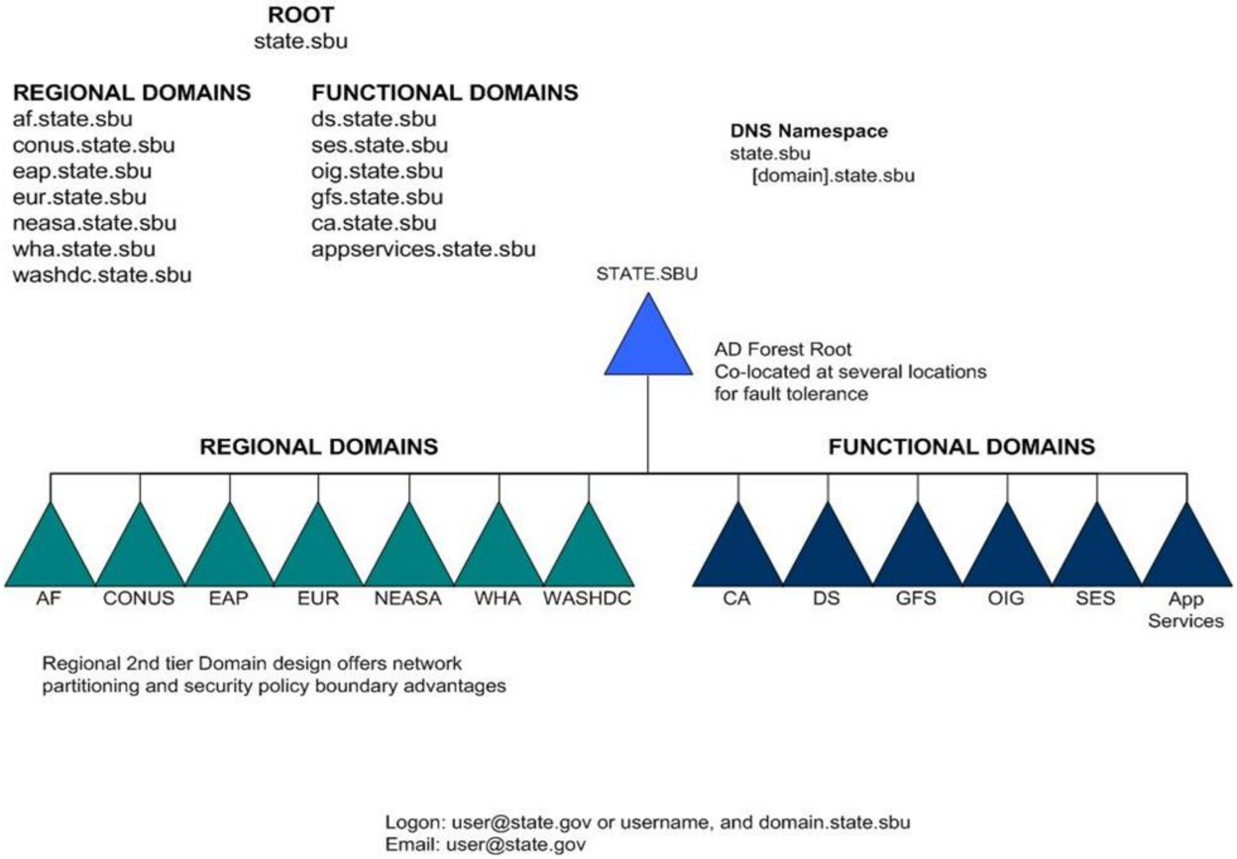
(U) Through another service, called Rights Management, organizations use AD to safeguard digital information from unauthorized use by allowing IT administrators to define who in the organization can open, modify, or take other actions related to the information. According to Microsoft, once a user account has received authentication and can potentially access an object, the type of access granted is determined by either the user rights that are assigned to the group (or user) or the access control permissions that are attached to the object. This AD concept, in some cases, provides single sign-on capabilities to certain systems and applications. Thus, for such systems and applications, some identity and authentication controls are inherited from AD.

(U) Department of State's Implementation of Active Directory

~~(SBU)~~ The Department has divided its AD structure into one root domain and 13 regional and functional domains (to include bureaus, offices, and posts). Each domain is further broken down by OU at the post and bureau level. The main purpose for the AD domain is to support the underlying physical and logical directory infrastructure with respect to administration and network replication. Domains provide partitions of the AD architecture (known as the forest) to allow for smaller AD databases to reside and replicate the domain-naming context separately from other domains. For an illustration of the Department's AD forest, including root state.sbu and all its subset domains (sometimes referred to as "child" domains), see Figure 1.

[10] **(U)** An object is a distinct, named set of attributes that includes shared resources, such as servers, shared volumes, and printers; network user and computer accounts; and domains, applications, services, and security policies. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/bb727067.aspx, accessed 8/26/2014.

(U) Figure 1. Department of State Active Directory Design Overview



(U) Source: Department, System Administrative Guide – Department Active Directory Design Overview.

(U) One of the biggest advantages of partitioning with domains is that a single large domain-naming context does not have to be replicated across slow links. Most of the traffic is eliminated and contained within the domain environment that would be located on the end-user side of the slow link.

(U) AD domains are also used to control replication, for example, when applying group security policy. From a domain perspective, all properties of all objects within the domain are replicated to all Domain Controllers[11] within that domain only. Further, Global Catalog servers contain a partial replica (all objects and selected properties) of all domains in the forest. To reduce the amount of domain data that is maintained in a Domain Controller (or to reduce the amount of domain data that is replicated to a Domain Controller), separate domains can be created. Although replication between sites is compressed and scheduled, initial replication to Domain Controllers in remote sites can be significant. Strategically locating Domain Controllers and Global Catalog servers can be used as an alternative to creating additional domains to

[11] **(U)** Domain Controllers are servers that store directory data and manage user and domain interactions, including user login processes, authentication, and directory searches. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/cc759623(v=ws.10).aspx, accessed 8/26/2014.

mitigate this issue. Global Catalogs are used for directory operations, such as logons and forest-wide searches, but replicated attributes can be limited.

(U) An AD domain is identified by a boundary of policy (such as authentication and domain-level security policies) and replication within an AD forest, and is distinguished by a unique namespace. Although some documentation would initially state that a domain is a security boundary, due to the tight integration of AD domains within the forest, this is not necessarily the case. The forest is the true security boundary.

(U) Due to the sensitivity of the forest design, network security is required at all times and locations/points. The distributive nature of AD requires fidelity or trust between servers and sub-networks within the forest. Improperly configured, implemented, or managed AD poses a risk to information security. Domain security is essential because multiple sites are merged into a single domain. Most Department offices prefer that users outside of their organizations do not have administrative access to their servers. If every administrator at a location within a domain were a Domain Administrator, this would be the case. The OU model in place within the Department's AD addresses this situation by enabling delegation of location administration through each location's OU Administrators group. The OU Administrator group in each OU has similar privileges to Domain Administrator for that specific OU only. OU Administrators have complete control over their respective OU hierarchy.

~~(SBU)~~ In order to access a network, a user must be uniquely identified and authenticated. Authentication is accomplished through passwords, token, biometrics, or a combination of these methods. To access the Department's OpenNet, a user must have a unique ID (username) and a password to authenticate. In a notice issued in April 2014, the Department announced plans to implement the use of personal identity verification cards at login to implement multifactor authentication.[12] Mandated by Homeland Security Presidential Directive 12,[13] personal identity verification will allow access to physical facilities and IT systems and increase security, reduce identify fraud, protect privacy, and improve the ability to provide reliable IT services.

(U) Prior OIG Reports

~~(SBU)~~ Since FY 2010, OIG has issued four reports[14] recommending improvements to the account management process in AD for the Department's OpenNet and ClassNet networks. Among other findings, each of the reports described inadequate account and identity management controls, which significantly increase the risk that information could be accessed

[12] **(U)** According to a Department Notice that was issued in April 2014, the Department plans to implement personal identity verification for 50 percent of domestic locations by September 30, 2014, and all remaining domestic and overseas personnel will be transitioned by the end of 2016.

[13] **(U)** Homeland Security Presidential Directive 12, issued August 27, 2004, requires mandatory, government-wide standards for secure and reliable forms of identification issued by the Federal Government to its employees and Federal contractors.

[14] **(U)** FY 2010 - 2013 State Federal Information Security Management Act Audits. These audit reports are as follows: OIG, AUD-IT-11-07, *Review of Department of State Information Security*, November 2010; AUD-IT-12-14, *Evaluation of the Department of State Information Security Program*, November 2011; AUD-IT-13-03, *Audit of Department of State Information Security Program*, November 2012; and AUD-IT-14-03, *Audit of Department of State Information Security Program*, November 2013.

and exploited for nefarious purposes. Each year, in its FISMA audits, OIG has reported findings related to the account management of AD involving issues such as identity and access management, but corrective actions have not been accomplished enterprise-wide.

(U) Objective

(U) To determine whether the Department has consistently implemented and overseen Active Directory Domain Services and Rights Management across the enterprise environment.

(U) Audit Results

(U) Finding A. The Department Has Successfully Implemented Active Directory Domain Services

(U) OIG found that IRM has organized and successfully implemented AD Domain Services in a standardized structure, including Group Policy Objects and trusts, and put procedures in place to better ensure business continuity. This is important because AD Domain Services stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

(U) IRM Has Implemented Group Policy Objects

(U) Group Policy Objects are configurations used to enforce settings on computers and to control the working environment of user and computer accounts to assist in reducing computer security risks. OIG found that IRM has established and enforced Group Policy Objects at the root domain to ensure required policies are not overridden at any lower level.

~~(SBU)~~ DS requires Domain Controllers to be configured to Department standards.[15] All Domain Controllers on the network are scored via iPost[16] to determine whether Department configuration standards are being met. OIG found that IRM had configured security settings through Group Policy Objects. Specifically, OIG reviewed Group Policy Objects for audit policy,[17] user rights assignments,[18] security options,[19] and event log policies,[20] determining that all of these configurations aligned with DS requirements.

[15] **(U)** The Bureau of Diplomatic Security provides Department System Administrators with security configuration standards that are mandatory for all servers operating within the Department.

[16] **(U)** iPost is the custom application that continuously monitors and reports risk on the IT infrastructure at the Department.

[17] **(U)** Audit policy is an important facet of information security. Configuring Audit policy settings that monitor the creation or modification of objects allows the tracking of potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach. Microsoft, *TechNet*, echnet.microsoft.com/en-us/library/dd349800(v=WS.10).aspx, accessed 8/26/2014.

[18] **(U)** User rights assignment is the location in which administrators govern user rights. User rights govern the methods by which a user can log onto a system, and these rights include logon rights and privileges. Microsoft, *TechNet*, Technet.microsoft.com/en-us/library/dd349804(v=ws.10).aspx, accessed 8/26/2014.

[19] **(U)** The security options section of Group Policy configures computer security settings for digital data signatures, administrator account names, access to floppy disk and CD/DVD drives, driver installation behavior, and logon prompts. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/dd349805(v=WS.10).aspx, accessed 8/26/2014.

(U) As it pertains to authentication, OIG also reviewed a Group Policy Object that addressed authentication. For example, Volume 12 of the *Foreign Affairs Manual* (FAM), Section 623.3-1, requires that a newly created password must be in accordance with the following specifications:

> **(U)** (1) Password length: The password must be a minimum of 12 characters in length. If the system which the user is accessing does not accommodate 12 characters, then the user should use the maximum number of character spaces available; and
>
> **(U)** (2) Password composition: The password must be composed of characters from at least three of the following four groups from the standard keyboard:
>
> > **(U)** (a) Upper case letters (A-Z);
> > **(U)** (b) Lower case letters (a-z);
> > **(U)** (c) Arabic numerals (0 through 9); and
> > **(U)** (d) Nonalphanumeric characters (punctuation symbols); and
>
> **(U)** (3) Thereafter, users should construct their own passwords when required: at least once every 60 days, and when it is suspected that the password has been compromised. The latter must also be reported to the Information System Security Officer (ISSO).

~~**(SBU)**~~ OIG found that the Department has implemented a Group Policy Object that applied to each user object on the network to ensure password specifications are followed. These authentication controls allow for increased security over user accounts.

(U) IRM Has Implemented Trusts

~~**(SBU)**~~ Trusts assist in managing communication between users and domains because they are authentication pipelines that must be present in order for users in one domain to access resources in another domain. OIG found that IRM has established transitive trusts[21] at the root domain, and changes to trusts are captured via ChangeAuditor.[22] Having this control in place allows personnel to be made aware of any unintentional or potential malicious changes in the trusts.

[20] **(U)** Event logs record events that happen on the computer. Examining the events in these logs can help trace activity, respond to events, and assist in keeping systems secure. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/dd349798(v=ws.10).aspx, accessed 8/26/2014.

[21] **(U)** Transitive trust means that the trust relationship extended to one domain is extended automatically to any other domain that is trusted by that domain. Transitive trust is applied automatically for all domains that are members of the domain tree or forest. Microsoft, *TechNet*, technet.microsoft.com/en-us/library/cc977993.aspx, accessed 8/26/2014.

[22] **(U)** ChangeAuditor is a tool used to assist IRM personnel in audits, alerting, and reports of changes in AD.

(U) IRM Has Implemented Business Continuity

~~(SBU)~~ Business Continuity is defined as the capability of an organization to continue delivery of products or services at acceptable, predefined levels following a disruptive incident.[23] Because directory data is stored using AD Domain Services, it is important that the data is backed up.[24] OIG found that IRM has established procedures and implemented business continuity practices that backed up the AD forest daily. Therefore, if data is inadvertently deleted following a disruptive incident, IRM has procedures in place to restore the data at an acceptable level.

(U) Finding B. Active Directory Rights Management Needs Governance Structure and Guidance

~~(SBU)~~ OIG found that IRM has not consistently implemented AD Rights Management, which is necessary to enforce IT security standards. OIG identified deficiencies related to IRM's oversight for review of user accounts, the frequency with which accounts are disabled or removed when no longer needed, and the OU structure of the user accounts. These deficiencies occurred because IRM has not established a governance structure to ensure that AD Rights Management is implemented and managed consistently. The Department's AD Rights Management is decentralized, allowing the ISSOs at each bureau or post to make decisions about implementing and overseeing AD accounts with insufficient guidance. Without a proper governance structure and guidance for AD Rights Management, the risk of unauthorized access or malicious activity on the network is significantly increased.

(U) Reviewing Accounts and Audit Reports

(U) National Institute of Standards and Technology Special Publication 800-53, Revision 3, states that to manage information system accounts, organizations should:

- **(U)** identify authorized users of the information system and specify access privileges
- **(U)** require appropriate approvals for requests to establish accounts
- **(U)** establish, activate, modify, disable, and remove accounts
- **(U)** notify account managers when information system users are terminated, transferred, or changed
- **(U)** deactivate accounts of terminated or transferred users
- **(U)** grant access to the system based on a valid access authorization and intended system usage
- **(U)** review accounts

[23] **(U)** Business Continuity Institute, "What is BC?" www.thebci.org/index.php/resources/what-is-business-continuity, accessed 8/26/2014.

[24] **(U)** A back-up is a copy of files and programs made to facilitate recovery, if necessary. NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*, May 2013.

~~(SBU)~~ OIG found that the Department's ISSOs did not consistently review all accounts to ensure that the user accounts were needed in relation to Rights Management. Specifically, we found that ISSOs reviewed AD user accounts at various frequencies, ranging from daily to quarterly. The purpose of these reviews is to identify aged accounts, expired accounts, and passwords that were set not to expire[25] and then take appropriate action. Additionally, not all AD user accounts were reviewed to ensure that only approved accounts were established. Specifically, there was no structure in place to prevent user accounts from being established without proper authorization by OU system administrators.

(U) Department guidance also requires ISSOs to review monthly audit reports (audit logs) produced by AD. Specifically, 12 FAM 629.2-7 states the following:

> **(U)** The ISSO must review monthly the audit reports for potential security-related incidents such as:
>
> > **(U)** (1) Multiple logon failures;
> > **(U)** (2) Logons after-hours or at unusual times;
> > **(U)** (3) Failed attempts to execute programs or access files;
> > **(U)** (4) Addition, deletion, or modification of user or program access privileges; or
> > **(U)** (5) Changes in file access restrictions.

~~(SBU)~~ The Domain Controller audit logs capture events on the network, and specific events are collected and made available for ISSOs, via iPost, so that they may review and identify security anomalies. OIG found that only half (6 of 12) of the ISSOs interviewed during this audit were aware that they had access to these Domain Controller audit logs to review the specific elements in 12 FAM 629.2-7, as discussed in the previous paragraph.

(U) Removing and Disabling Accounts

~~(SBU)~~ According to IRM data, the Department had 122,976 AD accounts as of March 19, 2014, which included primary and secondary users, service accounts, and mailboxes.[26] During the same March 2014 period, HR reported that the Department had 78,791 employees—a difference of 44,185.[27] Although some of the accounts may belong to either contractors or service accounts, OIG was unable to determine the reason for the significant difference between the number of AD user accounts and the number of employees reported by HR. OIG concluded, and IRM concurred, that some of the AD accounts are no longer needed.

[25] **(U)** Reviews to identify accounts with passwords set not to expire are required to be conducted as prescribed by the 12 FAM 622.1-3(j). This criterion explains that the data center manager and the system manager must ensure that the maximum password age must be set to 60 days; instances in which the account is set not to expire would mean that the password age could exceed 60 days.

[26] **(U)** OIG obtained documentation from IRM on March 19, 2014, that contained all OpenNet Active Directory Accounts.

[27] **(U)** Employee total retrieved from the HR Knowledge Center (http://hrkc.hr.state.gov/kclandingpage/DOSPerson.aspx) as of March 2014.

(U) The Department has documented a time frame for when accounts should be disabled due to inactivity in the FAM for ClassNet; however, they have not identified a specific time of inactivity for disabling accounts for OpenNet. According to 12 FAM 632.1-3, "The system administrator must ensure that accounts are temporarily disabled after 90 days of inactivity. Before reactivating the account, the user's supervisor must recertify in writing, e.g., via email or memo that the user still requires the account." OIG is of the opinion that the same criteria should be applied to OpenNet accounts.

~~**(SBU)**~~ In February 2014, after our audit began, the Chief Information Officer requested that all system managers review and remediate aged[28] AD accounts. As a result of the system managers' actions and IRM's reconciliation, 12,509 accounts were identified in IRM's May 2014 analysis.[29] IRM removed 4,152 aged accounts and disabled 973 aged accounts.[30] Although these actions were necessary and beneficial, OIG's analysis of the AD account listing provided by IRM revealed that additional unneeded accounts may still exist. For example, IRM reported action on only 5,125 accounts, and in March 2014, OIG had identified 15,634 accounts as aged.

(U) Organizational Unit Account Structure

(U) The Department of State Global Address List and AD Standardization Guidelines[31] provide the following instructions:

- **(U)** Primary User Accounts must be located in the **Users** OU within the site's OU structure.
- **(U)** Secondary User Accounts must be located in the **Admin Accounts** OU within the site's OU structure. Also, the manager field must be populated with the Primary User Account of the Secondary User Account's owner.
- **(U)** Service Accounts must be located in the **Service Accounts** OU within the site's OU structure. Also, the manager field must be populated with the Primary User Account who is responsible for its management.
- **(U)** Shared Mailbox Accounts must be located in a sub-OU of the Users OU within the site's OU structure. The sub-OU must also be named **MAILBOXES**. Also, the manager field must be populated with the Primary User Account who is responsible for its management.

~~**(SBU)**~~ OIG found that OU account structures were not set up in accordance with Department standards. Specifically, OIG found:

[28] **(U)** Aged accounts are accounts that have been inactive for 90 days or more.

[29] **(U)** Aged accounts identified by IRM personnel as of May 9, 2014, as a result of the Department Notice to remediate AD accounts.

[30] **(U)** Due to various circumstances (such as extended medical leave, maternity leave, long-term courses at FSI, etc.) accounts may be legitimately required and cannot be deleted from AD. These accounts that will ultimately be needed, but will not be accessed within 90 days, are disabled to avoid unauthorized access.

[31] **(U)** The Department of State Global Address List and AD Standardization Guidelines, ver. 1.3.1, February 24, 2012.

- ~~**(SBU)**~~ 2,865 of 122,976 AD accounts (2 percent) were not set up in accordance with the required OU account structure. These accounts were not located in the proper OU as prescribed by Department standards. Following these standards for OU account structure would ensure uniformity of AD user and computer account information and aid ISSOs to better track which users are within their purview. Without being able to easily identify and track the accounts, more accounts can go dormant and not be disabled. These dormant accounts can be the target of insider threats and external attacks.

- ~~**(SBU)**~~ 60 of 5,795 administrative accounts (1 percent) did not have a primary user associated with the account. Including a primary user name helps to easily identify who is responsible for management of the account, specifically for password management of the account. Administrator accounts have privileges that allow the user the ability to make changes and hide this activity.

~~(SBU)~~ Lack of AD Rights Management Governance Structure

~~**(SBU)**~~ The deficiencies OIG identified with AD Rights Management primarily occurred because IRM had not established a governance structure or strategy to ensure that AD Rights Management is implemented and managed consistently. Instead, AD Rights Management is decentralized, and the Information Management Officers at each bureau or post are allowed to make decisions about implementing and overseeing AD accounts. Having a governance structure is important so that IRM's IT strategy can be aligned with its business strategy and the Department's strategic goals. A governance structure is also essential to comply with numerous regulations related to IT accountability[32] prescribed by the National Institute of Standards and Technology, Office of Management and Budget, and Microsoft Best Practices, among others.

~~**(SBU)**~~ The lack of guidance related to AD Rights Management is also problematic. The FAM does not provide sufficient information regarding AD Rights Management. Moreover, IRM has not issued guidance to Information Management Officers to help identify, disable, or remove unneeded AD accounts. The Department lacks an overall strategy that provides policies and procedures for managing AD account management, and there is no centralized IRM enforcement mechanism in place to take appropriate action when bureaus and posts are not reviewing AD accounts monthly. In addition, IRM did not have a process in place to ensure that bureaus and posts updated the OU structure in accordance with IRM guidance. Further, due to competing priorities, IRM did not make improving AD Rights Management a priority. One initiative that could assist IRM to improve controls over AD Rights Management is the Department-wide use of personal identity verification cards for multifactor authentication. Personal identity verification cards are required by Homeland Security Presidential Directive 12, which provides mandatory, government-wide standards for secure and reliable forms of identification issued by the Federal Government to its employees and Federal contractors. This initiative is intended to increase security, reduce identity fraud, protect privacy, and improve the ability to provide reliable, secure IT services.

[32] **(U)** IT governance structure information derived from http://www.cio.com/article/2438931/governance/it-governance-definition-and-solutions.html accessed 7/2/2014.

~~(SBU)~~ Additional Risk and Associated Cost With Active Directory

~~(SBU)~~ Without a governance structure for AD account management, the risk of unauthorized access is significantly increased. Enabled AD accounts that are not properly managed—that are not reviewed and identified as aged, that have passwords that do not expire, or that have no required password, for example—become more vulnerable to unauthorized access. In FISMA audit reports released in 2012 and 2013,[33] OIG reported that the user accounts for terminated employees had been logged onto after the employees left employment. For example, in 2012, 6 of 384 terminated users tested logged into their accounts after their termination date, and in 2013, 4 of 25 sampled users logged into their accounts after their termination date. Unauthorized usage can lead to improper access to confidential data or malicious activities on the network.

~~(SBU)~~ There is also a financial incentive to disable or remove unneeded accounts. Based on discussions with Department personnel, there is an initial AD cost of $15.72 per object and an annual maintenance cost of $4.58 per object. As noted, the Department recently deleted approximately 4,152 accounts. If the Department had sufficiently managed its AD accounts, the Department would have avoided more than $19,000 in unnecessary maintenance costs for these accounts. Additional funds could be saved by removing other unneeded accounts. These funds could be used for other priorities within IRM.

~~(SBU)~~ This audit addressed only AD account management on OpenNet, but deficiencies in AD account management have been identified on both OpenNet and ClassNet each year since the FY 2010 Department of State FISMA audit. Therefore, the deficiencies identified in this audit are likely to exist on ClassNet as well.

> ~~(SBU)~~ **Recommendation 1.** OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Human Resources and Diplomatic Security, develop and implement an overall strategy that will provide policies and procedures for managing Active Directory account management that reflects the interaction between all Bureaus.
>
> ~~(SBU)~~ **Management Response:** IRM suggested the scope of this recommendation be expanded to include the Bureaus of Human Resources and Diplomatic Security.
>
> **(U) OIG Reply:** Because IRM did not indicate agreement or disagreement with the recommendation, OIG considers the recommendation unresolved. As requested by IRM and after consultation with HR and DS, we modified the recommendation to reflect the role of HR and DS as coordinating partners. This recommendation can be resolved when OIG receives and accepts a corrective action plan with milestones that addresses the recommendation. This recommendation can be closed when OIG receives and accepts evidence that IRM has developed and implemented a strategy that provides policies and procedures for managing Active Directory accounts.

[33] **(U)** OIG, AUD-IT-13-03, *Audit of Department of State Information Security Program*, November 2012, and AUD-IT-14-03, *Audit of Department of State Information Security Program*, November 2013.

~~(SBU)~~ Recommendation 2. OIG recommends that the Bureau of Information Resource Management update and implement Volumes 5 and 12 of the *Foreign Affairs Manual* to specifically address the deficiencies in Active Directory account management.

~~(SBU)~~ Management Response: IRM concurred with this recommendation and indicated that it had already taken steps to implement it. Specifically, IRM stated that 5 FAM 820 was updated on July 17, 2014, to incorporate guidance for aged accounts. A draft Global Address List and Active Directory Standardization Guide was being reviewed and will be published in the FAH. In addition, an "All Diplomatic and Consular Posts" telegram and Department notice would be promulgated once the new Foreign Affairs Handbook is published. IRM expects to have these actions completed by the end of the year.

(U) OIG Reply: OIG considers the recommendation resolved and notes that IRM has begun taking action to implement it. This recommendation can be closed when OIG receives and accepts evidence that IRM has updated the *Foreign Affairs Manual* to specifically address deficiencies in Active Directory account management.

~~(SBU)~~ Recommendation 3. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Human Resources and Diplomatic Security, develop and implement guidance that describes a sustainable and repeatable process for determining how to identify and then disable or remove unneeded OpenNet accounts, including users that are not Department of State employees, such as contractors and other Federal agencies.

~~(SBU)~~ Management Response: IRM concurred with this recommendation and suggested the scope of this recommendation be expanded to include the Bureaus of Human Resources and Diplomatic Security.

(U) OIG Reply: OIG considers the recommendation resolved and modified the recommendation to include HR and DS as coordinating partners, as requested by IRM. This recommendation can be closed when OIG receives and accepts evidence that IRM has developed and implemented guidance that prescribes a process for identifying, disabling, or removing unneeded OpenNet accounts.

~~(SBU)~~ Recommendation 4. OIG recommends that the Bureau of Information Resource Management develop and implement a process to ensure that Information Systems Security Officers conduct monthly reviews of audit logs for security anomalies, as prescribed by Volume 12, Section 629.2-7, of the *Foreign Affairs Manual*.

~~(SBU)~~ Management Response: IRM concurred with this recommendation and stated that the Office of Information Assurance has established a portfolio management system for ISSOs (for each geographic region including domestic), and acquired a data analytic tool called "Splunk" to provide technical capability. IRM intends to fully develop this tool within the next 12 months.

(U) OIG Reply: OIG considers the recommendation resolved because IRM has begun taking steps to implement it. This recommendation can be closed when OIG receives and accepts evidence that IRM has implemented a process to ensure ISSOs conduct monthly reviews of audit logs as prescribed by the *Foreign Affairs Manual*.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the Bureau of Information Resource Management develop and implement a process directing Organizational Unit Administrators to update their Active Directory organizational unit structure in accordance with the Department of State Global Address List and Active Directory Standardization Guidelines.

~~(SBU)~~ **Management Response:** IRM concurred with this recommendation and requested that it be modified to reflect the role the Information Management Officer has in developing guidance for ISSOs.

(U) OIG Reply: OIG considers the recommendation resolved and has modified the recommendation as requested. This recommendation can be closed when OIG receives and accepts evidence that IRM has implemented a process directing Organizational Unit Administrators to update their Active Directory organizational unit structures.

~~(SBU)~~ **Recommendation 6.** OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Diplomatic Security and Human Resources, implement the use of Personal Identity Verification cards—as detailed in the Chief Information Officer’s implementation plan for logical access—for all Department employees eligible for a National Agency Check and Inquiry, as required by Homeland Security Presidential Directive 12.

~~(SBU)~~ **Management Response:** IRM concurred with this recommendation and stated that it is working on a strategy to implement Personal Identity Verification cards for logical access on OpenNet. IRM indicated that it plans to complete this action after the first of the year.

(U) OIG Reply: OIG considers the recommendation resolved because IRM has begun taking steps to implement it. This recommendation can be closed when OIG receives and accepts evidence that IRM has implemented the use of Personal Identity Verification cards for all applicable Department employees.

(U) List of Recommendations

~~(SBU)~~ Recommendation 1. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Human Resources and Diplomatic Security, develop and implement an overall strategy that will provide policies and procedures for managing Active Directory account management that reflects the interaction between all Bureaus.

~~(SBU)~~ Recommendation 2. OIG recommends that the Bureau of Information Resource Management update and implement Volumes 5 and 12 of the *Foreign Affairs Manual* to specifically address the deficiencies in Active Directory account management.

~~(SBU)~~ Recommendation 3. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Human Resources and Diplomatic Security, develop and implement guidance that describes a sustainable and repeatable process for determining how to identify and then disable or remove unneeded OpenNet accounts, including users that are not Department of State employees, such as contractors and other Federal agencies.

~~(SBU)~~ Recommendation 4. OIG recommends that the Bureau of Information Resource Management develop and implement a process to ensure that Information Systems Security Officers conduct monthly reviews of audit logs for security anomalies, as prescribed by Volume 12, Section 629.2-7, of the *Foreign Affairs Manual*.

~~(SBU)~~ Recommendation 5. OIG recommends that the Bureau of Information Resource Management develop and implement a process directing Organizational Unit Administrators to update their Active Directory organizational unit structure, in accordance with the Department of State Global Address List and Active Directory Standardization Guidelines.

~~(SBU)~~ Recommendation 6. OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Diplomatic Security and Human Resources, implement the use of Personal Identity Verification cards—as detailed in the Chief Information Officer's implementation plan for logical access—for all Department employees who are eligible for a National Agency Check and Inquiry, as required by Homeland Security Presidential Directive 12.

(U) Appendix A

(U) Scope and Methodology

~~**(SBU)**~~ The Office of Inspector General (OIG), Office of Audits, performed fieldwork for this audit during February−July 2014, in the Washington, D.C., area. The objective of this audit was to determine whether the Department has consistently implemented and overseen Active Directory (AD) Domain Services and Rights Management across the enterprise environment. To perform the audit, OIG gathered documentation, interviewed Information System Security Officers (ISSOs) about their respective AD practices, and held discussions with personnel from the Bureaus of Information Resource Management (IRM), Human Resources, and Diplomatic Security. In addition, OIG obtained a data extraction of all Department AD accounts—a total of 122,976 accounts—to assess the Department's AD Rights Management practices. These accounts included user, secondary (administrators), service, and mailboxes. IDEA[1] was used to identify aged accounts, aged passwords, accounts with no expiration dates, and accounts established without the proper organizational unit structure. As OIG identified anomalies, IRM, to its credit, was reviewing and correcting AD accounts simultaneously, as detailed in Finding B.

(U) OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

(U) Work Related to Internal Controls

(U) OIG assessed the adequacy of internal controls by performing manual assessments of internal controls related to the areas audited. As a result, OIG gained an understanding of the effectiveness of the Department's implementation and oversight of AD Domain Services and Rights Management. OIG identified and discussed exceptions with IRM personnel to understand the reason for internal control challenges. Through conversations with IRM, OIG gained an understanding of the policies and procedures related to the Department's management of AD and learned how the Department implements and oversees AD Domain Services and Rights Management. On September 30, 2014, OIG held an exit conference with IRM. At the exit conference and in its written response to the draft report, IRM requested that we clarify responsibilities for managing AD in this report. We modified the report as appropriate to reflect the role and responsibility of the Information Management Officer in managing AD. Significant deficiencies we identified with the management of AD are presented in the Audit Results section of this report.

(U) Use of Computer-Processed Data

~~**(SBU)**~~ To assess the reliability of computer-processed data, OIG reviewed the listing of all AD accounts provided by IRM and compared the total number with the number of AD

[1] **(U)** IDEA is an auditing and analysis software (created by Auditmation Services, Inc) used to import and analyze large amounts of data.

accounts represented in iPost. OIG determined that the data was sufficiently reliable to support the conclusions and recommendations presented in this report.

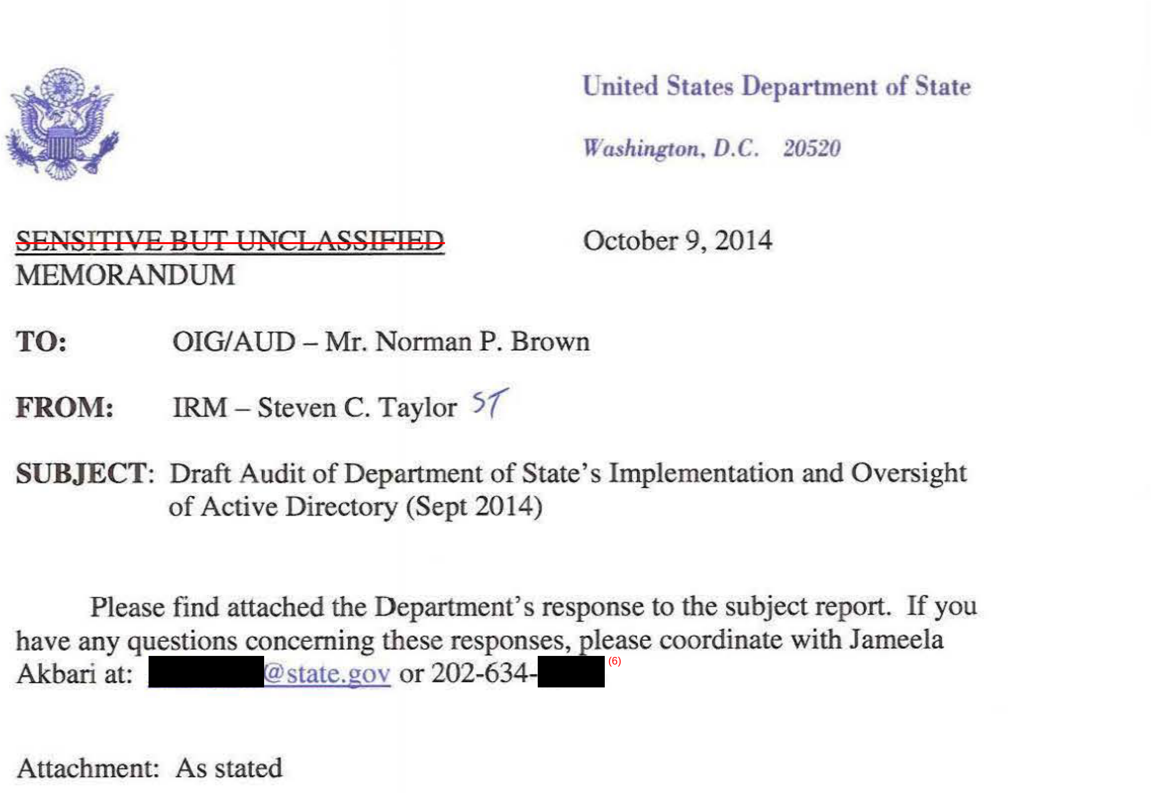
(U) Detailed Sampling Methodology

(U) OIG's sampling objective was to determine whether ISSOs were consistently implementing AD Rights Management across the Department. Due to the size of the Department and the number of ISSOs,[2] it was not feasible to discuss AD management practices with each ISSO. Therefore, OIG selected a sample of 18 ISSOs to interview. While 18 ISSOs were contacted, only 12 were available to discuss their AD management practices. The ISSOs were judgmentally selected based on the number of aged accounts within their domain. Specifically, OIG identified all aged user accounts within each domain, and further identified aged accounts by location (for each post and bureau). Within each domain, two ISSOs were selected—the ISSO with the highest number of aged accounts and the ISSO with the lowest number of aged accounts.

[2] **(U)** Based off the listing of ISSOs provided by IRM, there were approximately 318 primary ISSOs. This count does not include the number of alternate ISSOs.

(U) Appendix B

(U) Management Response



United States Department of State

Washington, D.C. 20520

~~SENSITIVE BUT UNCLASSIFIED~~

MEMORANDUM

October 9, 2014

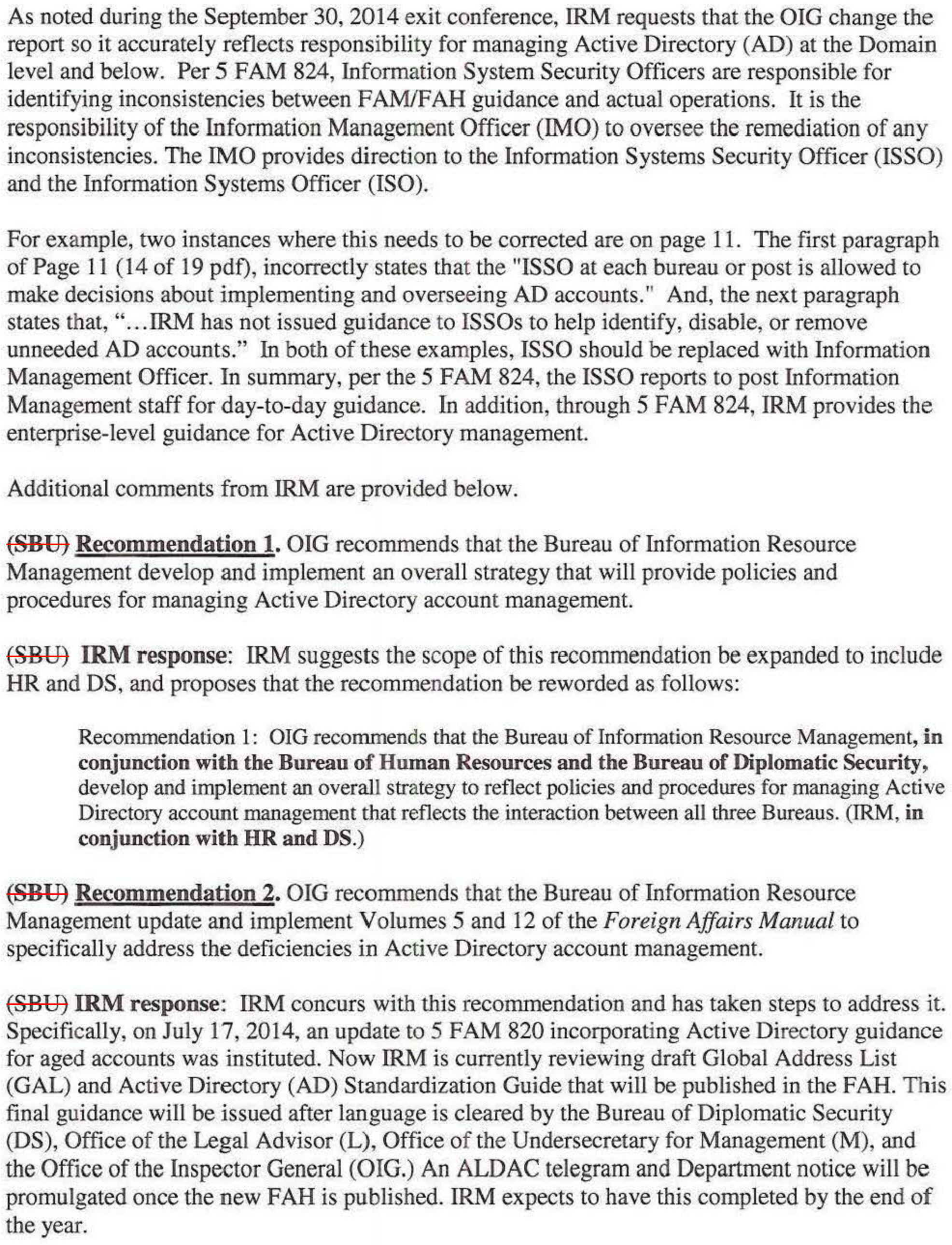
TO: OIG/AUD – Mr. Norman P. Brown

FROM: IRM – Steven C. Taylor ST

SUBJECT: Draft Audit of Department of State's Implementation and Oversight of Active Directory (Sept 2014)

Please find attached the Department's response to the subject report. If you have any questions concerning these responses, please coordinate with Jameela Akbari at: [redacted]@state.gov or 202-634-[redacted] (6)

Attachment: As stated



As noted during the September 30, 2014 exit conference, IRM requests that the OIG change the report so it accurately reflects responsibility for managing Active Directory (AD) at the Domain level and below. Per 5 FAM 824, Information System Security Officers are responsible for identifying inconsistencies between FAM/FAH guidance and actual operations. It is the responsibility of the Information Management Officer (IMO) to oversee the remediation of any inconsistencies. The IMO provides direction to the Information Systems Security Officer (ISSO) and the Information Systems Officer (ISO).

For example, two instances where this needs to be corrected are on page 11. The first paragraph of Page 11 (14 of 19 pdf), incorrectly states that the "ISSO at each bureau or post is allowed to make decisions about implementing and overseeing AD accounts." And, the next paragraph states that, "…IRM has not issued guidance to ISSOs to help identify, disable, or remove unneeded AD accounts." In both of these examples, ISSO should be replaced with Information Management Officer. In summary, per the 5 FAM 824, the ISSO reports to post Information Management staff for day-to-day guidance. In addition, through 5 FAM 824, IRM provides the enterprise-level guidance for Active Directory management.

Additional comments from IRM are provided below.

~~(SBU)~~ **Recommendation 1.** OIG recommends that the Bureau of Information Resource Management develop and implement an overall strategy that will provide policies and procedures for managing Active Directory account management.

~~(SBU)~~ **IRM response**: IRM suggests the scope of this recommendation be expanded to include HR and DS, and proposes that the recommendation be reworded as follows:

> Recommendation 1: OIG recommends that the Bureau of Information Resource Management**, in conjunction with the Bureau of Human Resources and the Bureau of Diplomatic Security,** develop and implement an overall strategy to reflect policies and procedures for managing Active Directory account management that reflects the interaction between all three Bureaus. (IRM, **in conjunction with HR and DS**.)

~~(SBU)~~ **Recommendation 2.** OIG recommends that the Bureau of Information Resource Management update and implement Volumes 5 and 12 of the *Foreign Affairs Manual* to specifically address the deficiencies in Active Directory account management.

~~(SBU)~~ **IRM response**: IRM concurs with this recommendation and has taken steps to address it. Specifically, on July 17, 2014, an update to 5 FAM 820 incorporating Active Directory guidance for aged accounts was instituted. Now IRM is currently reviewing draft Global Address List (GAL) and Active Directory (AD) Standardization Guide that will be published in the FAH. This final guidance will be issued after language is cleared by the Bureau of Diplomatic Security (DS), Office of the Legal Advisor (L), Office of the Undersecretary for Management (M), and the Office of the Inspector General (OIG.) An ALDAC telegram and Department notice will be promulgated once the new FAH is published. IRM expects to have this completed by the end of the year.

~~(SBU)~~ **Recommendation 3.** OIG recommends that the Bureau of Information Resource Management develop and implement guidance that describes a sustainable and repeatable process for determining how to identify and then disable or remove unneeded OpenNet accounts, including users that are not Department of State employees, such as contractors and other Federal agencies.

~~(SBU)~~ **IRM response**: IRM concurs with this recommendation and suggests the scope of this recommendation be expanded to include HR and DS. IRM proposes that the recommendation be reworded as follows:

> Recommendation 3: OIG recommends that the Bureau of Information Resource Management, **in conjunction with the Bureau of Human Resources, and the Bureau of Diplomatic Security,** develop and implement guidance that describes a sustainable and repeatable process for determining how to identify and then disable or remove unneeded OpenNet accounts, including users that are not Department of State employees, such as contractors and other Federal agencies. (IRM, **in coordination with HR and DS.)**

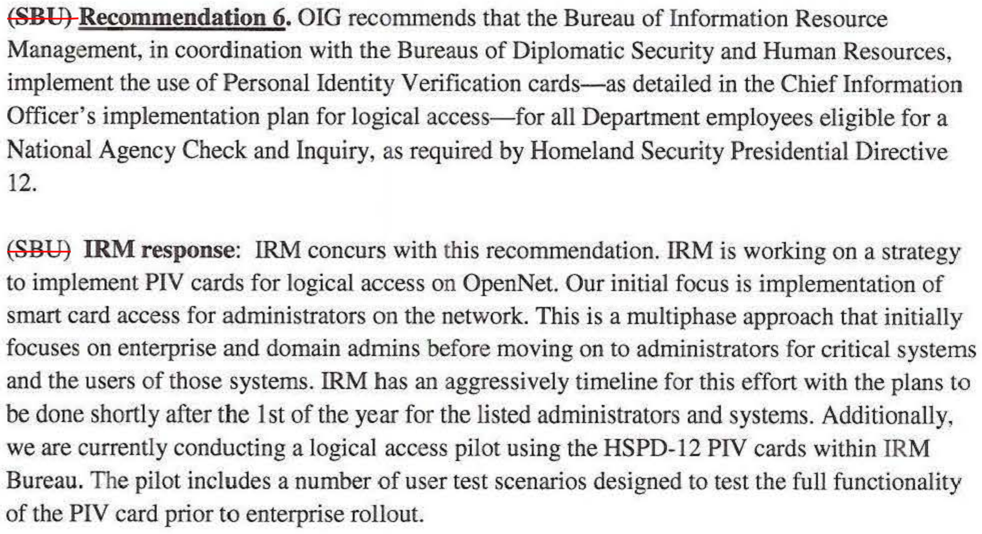
~~(SBU)~~ **Recommendation 4.** OIG recommends that the Bureau of Information Resource Management develop and implement a process to ensure that Information Systems Security Officers conduct monthly reviews of audit logs for security anomalies, as prescribed by Volume 12, Section 629.2-7, of the *Foreign Affairs Manual.*

~~(SBU)~~ **IRM response**: IRM concurs with the recommendation as written. This calendar year, the Office of Information Assurance established a portfolio management system for ISSOs worldwide, making use of ISSO Coordinators, essentially desk officers for each of the geographic regions as well as domestic ISSOs. This, combined with a recent year-end acquisition of a powerful Big Data analytics tool called "Splunk," will provide both the technical capability, as well as the desk officer resources, to fulfill this recommendation. It is IRM's intent to fully develop this within the next 12 months.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the Bureau of Information Resource Management develop and implement a process to ensure that Organizational Unit Administrators update their Active Directory organizational unit structure in accordance with the Department of State Global Address List and Active Directory Standardization Guidelines.

~~(SBU)~~ **IRM response**: IRM concurs with the general finding of this recommendation but asks that it be modified to reflect the role IRM has with developing guidance for ISSOs. As previously noted, overseas IMOs rather than ISSOs have responsibility for the administration of OpenNet and are part of the post's reporting structure. It is imperative that this distinction is made clear throughout the audit report, otherwise the critical separation of duties will become blurred.

> **(SBU) Recommendation 5.** OIG recommends that the Bureau of Information Resource Management develop and implement a process ~~to ensure that~~ **directing** Organizational Unit Administrators **to** update their Active Directory organizational unit structure in accordance with the Department of State Global Address List and Active Directory Standardization Guidelines.



~~(SBU)~~ **Recommendation 6.** OIG recommends that the Bureau of Information Resource Management, in coordination with the Bureaus of Diplomatic Security and Human Resources, implement the use of Personal Identity Verification cards—as detailed in the Chief Information Officer's implementation plan for logical access—for all Department employees eligible for a National Agency Check and Inquiry, as required by Homeland Security Presidential Directive 12.

~~(SBU)~~ **IRM response**: IRM concurs with this recommendation. IRM is working on a strategy to implement PIV cards for logical access on OpenNet. Our initial focus is implementation of smart card access for administrators on the network. This is a multiphase approach that initially focuses on enterprise and domain admins before moving on to administrators for critical systems and the users of those systems. IRM has an aggressively timeline for this effort with the plans to be done shortly after the 1st of the year for the listed administrators and systems. Additionally, we are currently conducting a logical access pilot using the HSPD-12 PIV cards within IRM Bureau. The pilot includes a number of user test scenarios designed to test the full functionality of the PIV card prior to enterprise rollout.

(U) Major Contributors to This Report

Jerry Rainwaters, Director
Division of Information Technology
Office of Audits

Jamie Horvath, Audit Manager
Division of Information Technology
Office of Audits

Kalina Blutcher, Auditor
Division of Information Technology
Office of Audits

Khafil-Deen Shonekan, Auditor
Division of Information Technology
Office of Audits

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT OF FEDERAL PROGRAMS HURTS EVERYONE.

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320
800-409-9926
oighotline@state.gov
oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219